The invention concerns a method for protecting a file with proprietary content against unauthorised copying by file sharing by other people's computers which are pooled to form an internet file sharing site and which make the file available in the form of randomly stored data records, each of which includes part of the proprietary content and metadata which inter alia consist of at least one hash ID and e.g. the title.

Considerable economic damage is caused to the owners of rights in particular to music and film works as well as games, due to unauthorised copying of the electronic versions of these works. A large proportion of unauthorised copying takes place by means of internet file sharing sites which work by the peer-to-peer (P2P) method. The commonest are central P2P file sharing sites in which on (central) servers are stored lists of contents available for exchange and the IP addresses of the computers subscribing to the file sharing sites, from which these contents can be downloaded. Upon a search inquiry, a subscribing computer receives from the answering server(s) a list with the IP addresses of those other subscribing computers which have stored a file with the desired content and are providing it for sharing. The searching computer then sets up connections to the providing computers and downloads the file with the desired content directly from the providing computers. In the case of decentralised P2P file sharing sites, upon search inquiries the subscribing computers also assume the role of the server for the searching computer and either answer that the file with the desired content is ready for downloading or, if not, pass on the search inquiry to other subscribing computers which if necessary in turn pass on until the file with the desired content is

found and the searching computer can download it from the subscribing computer concerned.

As a rule, the files provided for sharing are stored on several subscribing computers, this being in the form of individual data records, each of which includes a portion of the content and metadata which include at least one hash ID generated by the known hash method. The searching subscribing computer then downloads, from the subscribing computers providing the desired file and forming a group, the corresponding randomly stored data records and reassembles them into a file with the desired content again.

It is known that at least some owners of rights are trying to make this kind of unauthorised copying of their original files with proprietary contents difficult by participating in the relevant file sharing sites as providers, this being with files which apparently have the desired, proprietary content, but in actual fact contain only noise, parts of the title or the like. Although these unusable files, because they cannot be recognised as such with the aid of their metadata, broadcast themselves in the same way as the original files on the subscribing computers logged on to the file sharing site concerned, and are entered in the lists of the file sharing site servers, only the time needed for unauthorised copying of the original file can be prolonged by this so-called flooding method, because the user of the searching computer which, after downloading a file including at least one unusable data record, recognises this file as generally unusable, will start a new search and sooner or later obtain the desired original file from other file sharing site computers.

It is the object of the invention to provide a method of the kind indicated hereinbefore, which offers improved protection of files against unauthorised copying by a P2P method.

This object is achieved with a generic method according to the invention by the following steps:

1.1 searching for the content to be protected on the internet

1.2 saving at least the hash ID of each data record provided as a hit by at least one other person's computer

1.3 generating a data record which is modified from the data record provided and which includes at least the saved hash ID and replacement content data linked to the latter

1.4 answering inquiries from other people's computers about the file to be protected, by providing the modified data record.

The above-mentioned other people's computers can be both file sharing site servers and, particularly in the case of the decentralised P2P method, computers subscribing to the internet file sharing site concerned. Accordingly, provision of the modified data record as mentioned in step 1.4 above may be confined to the information that the requested file or part of it is ready for downloading from one's own computer, or provision may include release of downloading of the modified data record.

If the user of the other person's computer visually or acoustically tracks downloading of the file sought and requested by him, he will establish that he is receiving an unusable file instead of the desired file and so repeat the process or start a new search, If the user of the computer

does not track downloading, in his place the file sharing program of his computer will recognise, at the latest on completion of downloading, that the downloaded file includes at least one data record which has been modified from the original data record and so download the file again, or at least the data record concerned, or search for another (file sharing site) computer which will provide at least the data record concerned. Because the modified data record, without being recognisable as such at the outset, is available from many other computers subscribing to the file sharing site under supposedly the correct hash ID, there is a high probability that the searching and requesting computer will again download the modified data record, recognise it as modified, download it again or search, etc. After a certain time the user of this computer will break off the search for the original file.

Unlike the known flooding method of which the effectiveness, at least with certain file sharing programs, is limited by the fact that in the further search the user of the other person's computer can suppress the IP addresses of computers from which his computer has downloaded at least one unusable data record, with the method according to the invention the other person's computer constantly attempts again to download the original file again as soon as he has established that the previously downloaded file includes at least one data record which has been modified from the original data record.

The above-mentioned step 1.1 of the method according to the invention can appropriately be carried out in the following partial steps:

2.1 entering at least one search term identifying the file to be protected, in a local database of one's own computer

2.2 determining, entering and saving IP addresses of at least some of the other people's computers in the local database of one's own computer

2.3 setting up a connection of one's own computer to the internet and starting the search by scanning for the search term on the other people's computers.

The search term mentioned in step 2.1 may be in particular the title or part of the title of the proprietary content of the file, the interpreter, the author or a combination thereof. The determination and entry of IP addresses particularly of file sharing site servers mentioned in step 2.2 can be done manually, but in particular automatically using a suitable known search engine, with the aim of obtaining one or more lists of IP addresses from other people's computers subscribing to one or more file sharing sites.

One's own computer can then provide the modified data record belonging to the file to be protected, for downloading by the other people's computers designated by the saved IP addresses if the other person's computer concerned is a file sharing site server for inclusion in its list or, if the other person's computer is a subscribing computer, as a reply to its search inquiry about the file to be protected, which can then be followed by actual downloading of the (modified) data record.

Appropriately, the hash ID of each data record provided by another person's computer as a hit is compared with the saved hash IDs, and hits for which the result of

comparison is positive are not further processed into a modified data record, to avoid redundancy.

Defensive measures by the file sharing site can be rendered ineffective by regularly altering the IP address of one's own computer, to prevent the other people's computers from skipping this IP address after unsuccessful downloading of a data record from one's own computer.

Inquiries by other people's computers about the file to be protected, or alternatively just retrievals of the modified data record, can be logged, this being in anonymous form, in the event that this is necessary for reasons of data protection. The log can be processed under any classification aspects, that is, not only for every protected file, but also, if the method is performed by a third party on behalf of several owners of rights, according to owner of rights who as a rule has an interest in the protection of more than one file with proprietary content against unauthorised copying.

Furthermore, the method can be designed such that searching for the content to be protected is done only up to a predetermined expiry date, because in many cases, e.g. when the proprietary content is a current pop song, the interest in unauthorised copying of a file is limited to a distinct length of time.

The sequence of the method according to the invention is shown as an example in the drawings. They show:

Fig. 1   a flow chart of the search for files with proprietary contents provided by a file sharing site, and subsequent generation of a modified data record for each answer/hit.

Fig. 2   a flow chart of provision of the modified data record.

Patent claims

1. Method for protecting a file with proprietary content against unauthorised copying by file sharing by other people's computers which are pooled to form an internet file sharing site and which make the file available in the form of randomly stored data records, each of which includes part of the proprietary content and metadata which inter alia consist of at least one hash ID and e.g. the title, characterised by the following steps:

   1.1 searching for the content to be protected on the internet

   1.2 saving at least the hash ID of each data record provided as a hit by at least one other person's computer

   1.3 generating a data record which is modified from the data record provided and which includes at least the saved hash ID and replacement content data linked to the latter

   1.4 answering inquiries from other people's computers about the file to be protected, by providing the modified data record.

2. Method according to claim 1, characterised by the following partial steps in step 1.1:

   2.1 entering at least one search term identifying the file to be protected, in a local database of one's own computer

   2.2 determining, entering and saving IP addresses of at least some of the other people's computers in the local database of one's own computer

2.3 setting up a connection of one's own computer to the internet and starting the search by scanning for the search term on the other people's computers.

3. Method according to claim 2, characterised in that one's own computer provides the modified data record belonging to the file to be protected, for downloading by the other people's computers designated by the saved IP addresses.

4. Method according to any of claims 1 to 3, characterised in that the hash ID of each data record provided by another person's computer as a hit is compared with the saved hash IDs, and hits for which the result of comparison is positive are not further processed into a modified data record.

5. Method according to any of claims 1 to 4, characterised in that the IP address of one's own computer is regularly altered.

6. Method according to any of claims 1 to 5, characterised in that inquiries by other people's computers about the file to be protected are logged in anonymous form.

7. Method according to any of claims 1 to 6, characterised in that searching for the content to be protected is done only up to a predetermined expiry date.

Figure 1

1. Mark/remove expired search words
2. Enter
    - search words
    - period of protection
    - IP addresses of file sharing site servers
3. Database (DB)
4. Start
5. Read list of search words from DB
6. Read IP addresses of servers from DB
7. Connect to the servers
8. Search with search word from list of search words
9. Compare answers/hits with DB lists. Add new IP addresses to the database
10. Remove from list of hits
11. Is there a hash ID?
12. yes
13. no
14. Generate replacement content for hash ID
15. Save modified data record
16. End of hit list?
17. End of list of search words?
18. End

Figure 2

1. Start
2. Read IP addresses of file sharing site servers from the DB
3. Read list of modified data records from DB
4. Connect to the file sharing site servers and send list of modified data records
5. Wait for inquiries and send corresponding modified data records
6. Store inquiries in DB
7. Database (DB)